Secured Smart Home using Blockchain Technology

1st **S. B. Gopal,** *Department of Electronics and Communication Engineering*, *Kongu Engineering College*, *Anna University*, India, gopal.ece@kongu.ac.in

2nd **C. Poongodi,** *Department of Information Technology, Kongu Engineering College, Anna University*, India, poongs@kongu.ac.in

3rd **D. Nanthiya,** *Department of CT-UG, Kongu Engineering College, Anna University*, India, nanthiya.ctug@kongu.ac.in

4th **A. Jeevanantham**, *Department of Information Technology, Kongu Engineering College, Anna University*, India, jeeva@kongu.ac.in

5th **D. Sumithra,** *Department of Electronics and Communication Engineering, Kongu Engineering College, Anna University*,India,sumidass.nkl@gmail.com

6th **P. Tharani**, *Department of Electronics and Communication Engineering*, *Kongu Engineering College, Anna University*, India,tharani1101@gmail.com

7th **S. Umasri**, *Department of Electronics and Communication Engineering*, *Kongu Engineering College, Anna University*, India,umasris1999@gmail.com

Abstract— *IoT is one of the technology plays a vital role in today's world. Nowadays IoT devices are used all over the world. It has many features such as Intelligence, Connectivity, Dynamic nature, Enormous scale, Sensing, Heterogeneity and Security. Among these features, security is the most important one, which is implemented in most of the IoT devices using some technology. Blockchain technology is also used for implementing security in various devices. One block is linked with the other block which has a separate unique hash value. Where encryption is used in an organization to keep the data secure. By the sender the encrypted data is encoded. This technology works based on consensus algorithm by creating a new block and stores the information in this new block. It is also used for secure transactions between users without the help of third parties. Before the transaction added to the Blockchain it check for the validation using consensus algorithm. Consensus algorithm is essential for the Blockchain network because it maintain the integrity, reliability and security of the distributed system. And implementation of Blockchain involves installation of various packages such as npm and pip packages In this project we had combined a new mechanism with Blockchain which is Smart contract. By using smart contract, transactions could occur without third parties and unknown persons cannot data retrieve data stored without public/private keys. Here we designed a Home Automation Control with the help of Blockchain and smart contract, which controls the ON, and OFF state of the devices available in smart home. The result of this design was observed using GPIO emulator.*

Keywords— Blockchain, Smart contract, Transaction, Security.

I. INTRODUCTION

IoT is a collection and exchange of data in an object, which is associated with electronics, software and sensors. IoT integrate Computer based system and Remote control based system by which objects to be sensed and controlled. We are going towards IoT because it is a combination of sensor, connectivity, people and processes. Even though IOT provide service to all application, it has some challenges in Power consumption and Security. IoT has the ability to interconnect global information and communication infrastructure. It provides things related service such as interpretation between physical things and virtual things. In order to provide interconnectivity among various devices IoT uses different hardware and network platforms. Minimizing the power consumption by modifying the trickle timer algorithm plays a major role [23]. These devices are not stable in all circumstance (i.e. dynamic changes occur such as connected/disconnected). In order to provide efficient data handling, the number of devices which used for handling/managing purpose should be in order greater than number of devices connected. IoT plays a vital role in the technology. Gaining network and producing data are performed by Accessibility and Compatibility. The layers in IoT are Smart Device/Sensor Layer, Gateway and Networks Layer, Management Service Layer, Application Layer. Smart Device Layer provides services in terms of Wi-Fi , Ethernet, Bluetooth, Infrared . Wi-Fi, Ethernet, GSM, LTE is also provided by Gateway Network of Gateway and Network Layer. Management Service Layer provides Business Process Execution, Business Process Modeling, Virtual Entity etc. Application Layer is used for IoT applications. IoT has not only layers but also has technology. These technologies are categorized into three groups such as First group, Second group and Third group. Technologies in the first group impact devices such as microchip. Second group comprises some technologies which support network related services such as network sharing, address capacity. Technologies in third group have impact on management services and IoT applications. IoT has many features such as Intelligence, Connectivity, Dynamic Nature, and Enormous scale, Sensing, Heterogeneity and Security. It also built on several areas in place of Information management, Risk management, Security and it has some technology. These technologies are categorized into three groups such as First group, Second group and Third group. Technologies in the first group impact devices such as microchip. Second group comprises some technologies which support network related services such as network sharing, address capacity. Technologies in third group have impact on management services and IoT applications. RPL (Routing Protocol for Low Power and Lossy Networks) is a universally accepted routing protocol for IoT. By modifying the objective function of RPL, energy consumed can be minimized [24].

II. BLOCKCHAIN

Blockchain is a form of data structure, which records the transaction details, and the records are stored into the blocks. It is difficult to change or alter the information which is stored on Blockchain. This information's are open to all who are in the network because it is a distributed ledger and ensure the security, transparency and decentralization and also allows the resulting

ledger to accessed by different servers. Security issues play the main role while moving from wireless sensor networks to IoT [25].

One block is linked with the other block which has a separate unique hash value. Data security is a main concept involved in blockchain. Where encryption is used in an organization to keep the data secure. By the sender the encrypted data is encoded. After making some changes only it will send out of network to reach the destination and only authorized parties will allowed to access the information. In blockchain, the same concept is used. When someone wants to steal the information from the block, it is not possible. Because the unique hash value attached to a block will automatically get modified when other parties involved. When the hash value matches that authorized persons only allowed to use information.

Before the transaction added to the blockchain it check for the validation using consensus algorithm. If it satisfies that transaction is a valid version, it is added to the Blockchain. Bitcoin and ethereum network are based on Blockchain technology. It allows Bitcoin and other crypto currencies to operate without any central authority.

A. *Types of Blockchain*

Public Blockchain	It is used in Bitcoin, Ethereum, Litecoin
Private Blockchain	It is used in Multichain, Hyperledger, corda
Consortium Blockchain	It is used in Energy web foundation
Hybrid Blockchain	It is used in Dragonchain

B. *Advantage of Blockchain*

- Without the help of third parties, Block chain technology allows for verification.
- With help of smart contract, businesses can set a pre-condition on the blockchain. If the condition met, the transaction triggered automatically.
- Less cost and improve efficiency.
- It is open source and decentralized.

C. *Consensus Algorithm*

Consensus algorithm is used in blockchain. It is a kind of decision making process, where all the parties of the blockchain network come in contact with the common agreement about the present state of the distributed ledger. Consensus algorithm is essential for the blockchain network because it maintain the integrity, reliability and security of the distributed system. It built the trust between the unknown peers in the distributed computing system and then Proof-of-Work and Proof-of-Stake are most widely used mechanisms to reach consensus. In this it is important that

each block added to the network must follow the set of consensus rules. If the blocks fails to follow these consensus rules it will be removed.

III. SMART CONTRACT

Smart contract is a digital asset works between two or more parties, which is stored on the blockchain platform and has some agreement that is written in the form of codes. When the predetermined terms and condition meets, the smart contract automatically execute and provide the output. Ethereum is a platform that is build specifically for creating smart contract. Smart contract used to exchange money, property, data, shares or anything which are transferable without help of any third parties. Data stored in the blockchain cannot be changed or deleted. If one party not complete its duty, the other will be protected by the conditions of the smart contract. Smart contract is self verification, self executable and tamper proof. Smart contract has accuracy, low cost, clear communication, transparency, security, speed and efficiency.

Smart contract is formed through Byzantine fault-tolerant algorithm through decentralisation. Implementation of smart contract includes various mechanisms such as Bitcoin, Ethereum and Ripple. It actually run on blockchain so that data stored in public database cannot be changed easily. There are so many smart contract mechanism based on blockchain. Out of these top five things are Ethereum, NEM, NEO, cardano and Hyperledger. Another important thing in smart contract is code that deployed in blockchain are immutable which is not changed.

Solidity is used for implementing smart contract. It is a high level language and object oriented language. It has a similar syntax of java script language. With help of solidity, contract can be created by writing a code. It is used to enhance the Ethereum Virtual Machine (EVM). Solidity is statically typed, support inheritance libraries and complex user defined types among other. Solidity code filename has an extension of .sol and can be compiled using online compiler called remix or offline compiler called truffle. The compiler generates a byte code which run on Ethereum Virtual Machine in ethereum blockchain.

IV. WORKING AND ITS PERFORMANCE

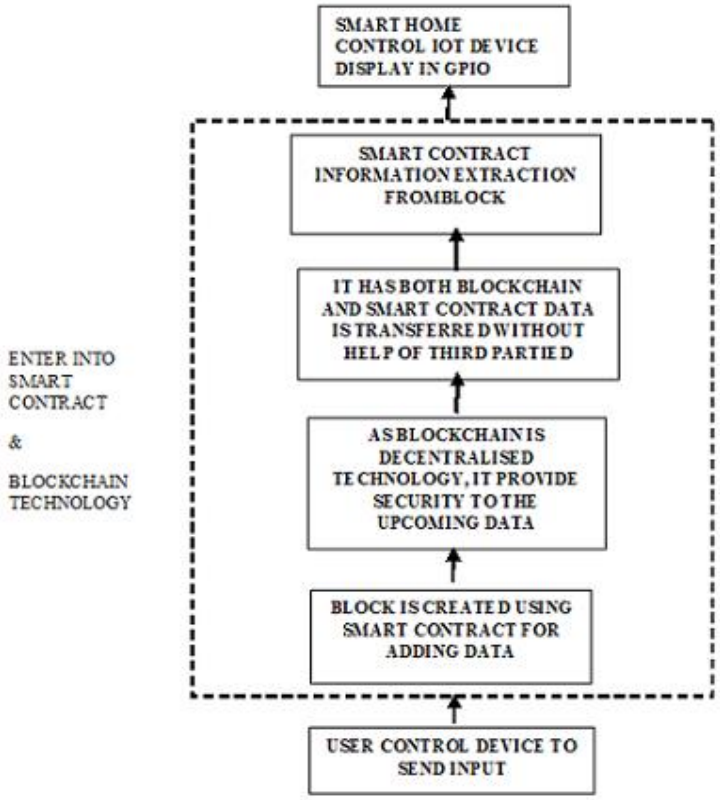
IoT is a technology used worldwide by the company, industries, they implement this technology in most of the devices according their usage. Those IoT implemented devices has many features among that one of the feature is Security.This security mechanism is implemented by using Blockchain technology. Blockchain is used to record the transaction details and store the information in the blocks. Each block can able to store 60 more inforamtion. As it is a decentralised one, it is difficult to change or alter those information which is stored on blockchain. Consensus algorithm is used in blockchain technology. We can make each and every transaction without the help of third parties.

In the home automation control implementation of blockchain involves installation of some pre-requesties and packages such as Npm and pip packages. Npm packages are Truffle, pip, Ganache. Truffle is used to link the Smart contract with the blockchain technology. pip is used for

using python language as it has so many inbuild functions. Ganache cli is used for mined transactions it can eliminate the overhead during transaction. Pip packages are Flask, Web3, GPIO Emulator. Flask is used for display of the webpages and it is based on the python language. Web 3 is used to combine the internet and the computer. GPIO emulator is used to show the pin of the home devices. Ethereum is a platform that is used for creating smart contract. Finally Smart contract is created using solidity. It has some predefined agreement written in code.

After installation of pre-requesties, Npm packages and pip packages,we create a smart contract. To deploy the Smart contract truffle is installed and used. The output of the Home automation control are observed using GPIO emulator and it is linked with ganache cli and pip by using the IP address. In the GPIO emulator we can observe the state of the devices which is 0 or 1 and the other window shows the ON and OFF state of the devices. The ON and OFF state webpage was obtained by using the browser. Details of the device state transaction are clearly displayed in the command prompt by using the IP address. For each transaction gas limit and gas price value is obtained and status of the every pin was also obtained.

Devices of Air quality sensor GPIO pin 1, Infotainment GPIO pin 2, Smart energy meter GPIO pin 3, Smart lock GPIO pin 4, Smart switch GPIO pin 5, Garden Springler GPIO pin 6, Garden light GPIO pin 7, TV switch GPIO pin 8, Computer switch GPIO pin 9, Home theatre GPIO pin 10, Camera control GPIO pin 11, Alarm system GPIO pin 12, Main gate GPIO pin 13, Front door GPIO pin 14, Hall light GPIO pin 15, Hall fan GPIO pin 16, Room 1 fan GPIO pin 17, Room 1 light GPIO pin 19, AC GPIO pin 18 and Room 2 Fan GPIO pin 20 state are observed.



From this figure, it shows that user had control the devices in the smart home automation using combined technology of block chain and smart contract. Here user had given the input using mobile/any interwork conected devices to send input to the destination. After that the given input is entered into the combined smart contract and blockchain technology. There, a separate block is created using smart contract where we can store 60 more information. As blockchain is a decentralized one, it is difficult to change or alter those information which is stored on blockchain. Consensus algorithm is used in blockchain technology. And the data stored here are transferred without the help of third parties. Flask is used to extract the input and it is send to the smart home devices.

By using combined technology of blockchain and smart home we can make transactions without the help of third parties. We can use switch and sensors for implementing on real time hardware. And the advantage of this technology is if any intruder changes the input given by the client, we can able to know the details of the intruder, Hence we can able to know the changes that occurred and the intruder who make that particular change.

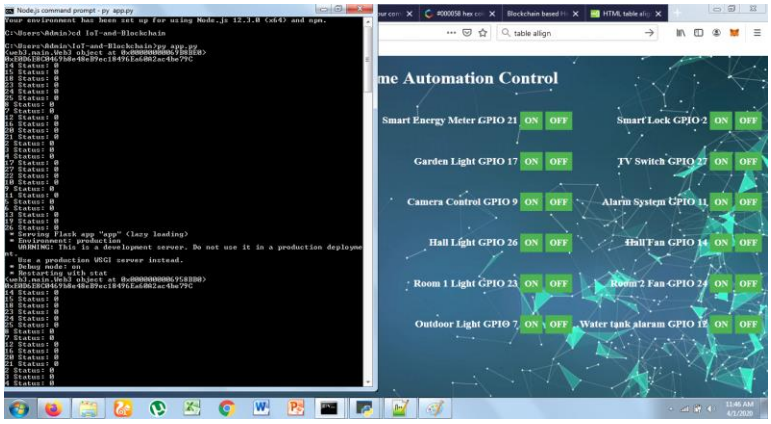


Fig. 1. It shows that the state of the device in windows prompt and GPIO emulator, while simulating in windows prompt using Node.js and npm.

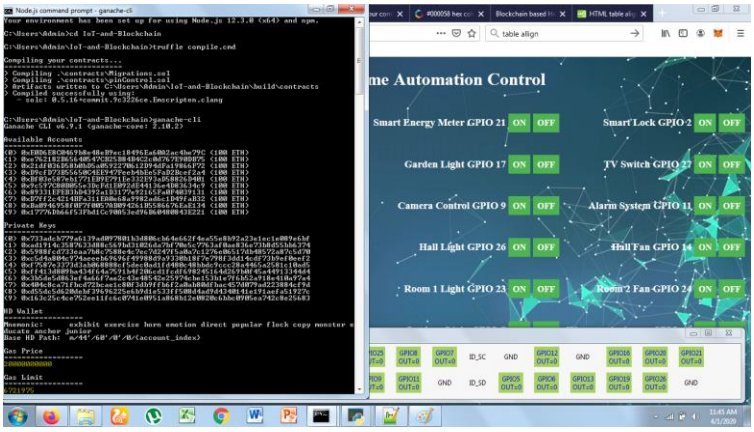


Fig. 2. It shows that the compilation of the contracts and address of the device in ganache cli, which links to the GPIO emulator for, output display.

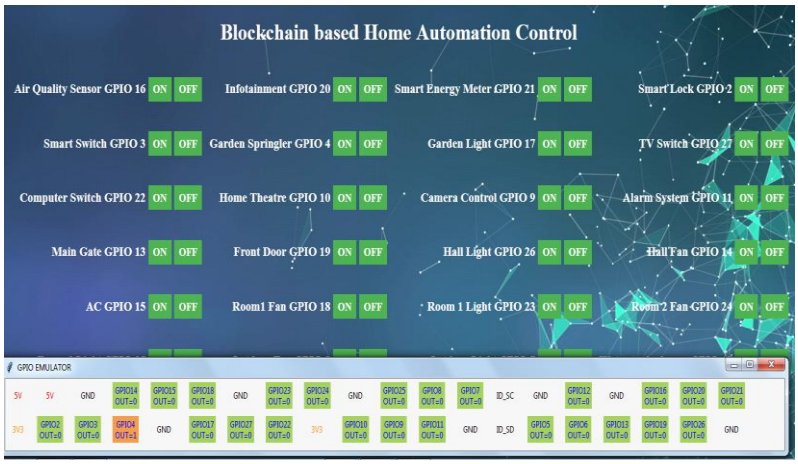


Fig. 3. It shows that if any of the device state is ON it changes the corresponding pin value to 1 in GPIO emulator. If any of the device state is OFF it changes the corresponding pin value to 0 in GPIO emulator.

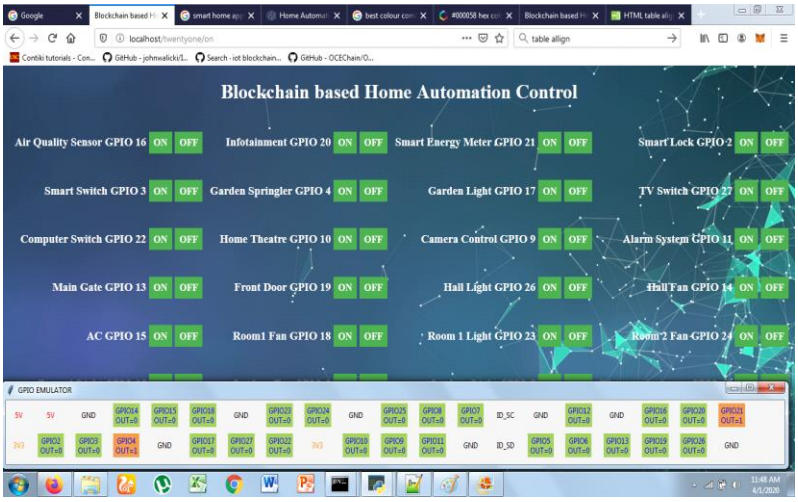


Fig. 4. This figure shows that if any of the device state is ON it changes the corresponding pin value to 1 in GPIO emulator. If any of the device state is OFF it changes the corresponding pin value to 0 in GPIO emulator.

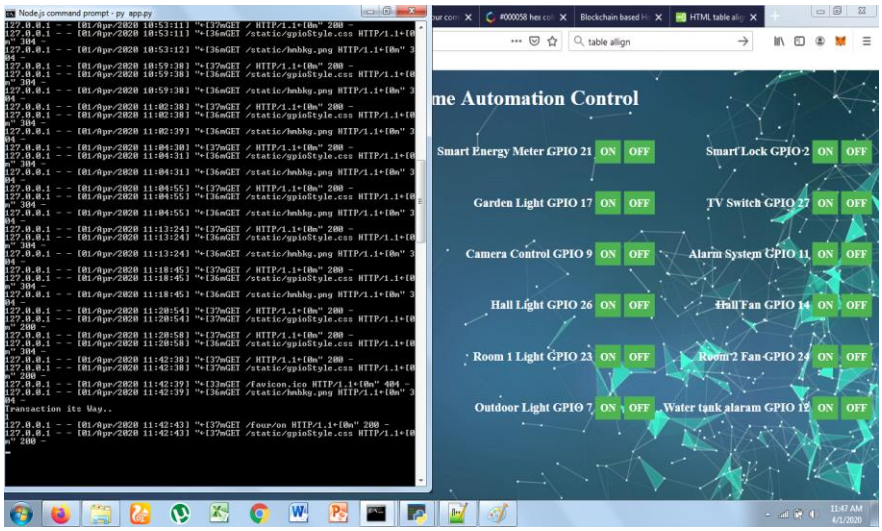


Fig. 5. It shows the simulation of the smart contract in command prompt by running py app.py.

V. CONCLUSION AND FUTURE WORK

The secured control of the smart home devices using Blockchain combined Smart contract technology was successfully observed using GPIO emulator. The ON and OFF state observation of Air quality sensor, Infotainment , Smart energy meter, Smart lock, Smart switch, Garden Springler, Garden light , TV switch, Computer switch, Home theatre, Camera control, Alarm system, Main gate, Front door, Hall light, Hall fan, Room 1 fan, Room 1 light, AC and Room 2 Fan devices are observed here. As this combined technology is implemented for secured control for change of devices state and the future work is to implement this existing in IOTA blockchain technology.

REFERENCES

[1]. Ali Dorri, Salil S.Kanhere, Raja Jurdak, Praveen Gauravaram(2019), 'LSB:A Lightweight Scalable Blockchain for IoT security and anonymity',Journal of Parallel and Distributed Computing, Vol 134, pp 180-197.

[2]. Anshul Anand, Mauro Conti, Pallavi Kaliyar, Chhagan Lal(2019), 'TARE:Topology Adaptive Re-kEying scheme for secure group communication in IoT networks',Wireless Network.malicious.

[3]. Bruno Bogaz Zarpelaoa, Rodrigo Sanches Mianib,Claudio Toshio Kawakania,Sean Carlisto de,Alvarengaa(2017), 'A Survey of intrusion detection in internet of things',Journal of Network and Computer Applications, Vol 84,pp 25-37.

[4]. David Airehrour, Jairo A.Gutierrez, Sayan Kumar Ray(2019), 'SecTrust -RPL:A Secure

trust-aware RPL routing protocol for internet of things',Future generation Computer Systems,Vol 93,pp 860-876.

[5]. Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis(2019), 'A systematic literature review of blockchain-based applications: Current status, classification and open issues',Telematics and Infomatics, Vol 36,pp 55-81.

[6]. Gauhar Ali, Naveed Ahmad, Yue Cao, Muhammad Asif, Haitham Cruickshank, Quazi Ejaz Ali(2019), 'Blockchain based permission delegation and access control in Internet of Things(BACI)', Computers and Security, Vol 86, pp 318-334.

[7]. Ghada Glissa, Aref Meddeb(2019), '6LowPSec: An end-to-end security for 6 LoWPAN', Ad Hoc Networks,Vol 82,pp 100-112.

[8]. Haiping Si, Changxia Sun, Yanling Li, Hongbo Qiao, Lei Shi(2019), 'IoT information sharing security mechanism based on blockchain Tehnology',Future Generation Computer Systems, Vol 101, pp 1028-1040.

[9]. Henane Lamaazi, Nabil Benamar(2020), 'A Comprehensive survey on enhancements and limitations of the RPL protocol:A focus on the objective function',Ad Hoc Network,Vol 96.

[10]. Imran Makhdoom, Mehran Abolhasan, Haider Abbas, Wei Ni(2019), 'Blockchain Adoptation in IoT: The challenges and a way forward', Journal of Computer and Network Applications, Vol 125,pp 251-179.

[11]. Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit(2020), 'A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT',Journal of Computer and Network Applications, Vol 149, pp 102-481.

[12]. Jun Lin, Zhiqi Shen, Chuyan Miao, Siyuan Liu (2017),"Using blockchain to build trusted lorawan sharing server", International Journal of Crowd Sciences, Vol. 1 No. 3, pp.270-280.

[13]. Jung Young Kim, Wen Hu, Dilip Sarkar, Sanjay Jha(2019), 'Long-term secure management of large scale Internet of Things applications', Journal of Network and Computer Applications, Vol 138, pp 15-26.

[14]. Maha Bouaziz, Abderrezak Rachedi, Abdelfettah Belghith(2019), 'EKF-MRPL:Advanced mobility support routing protocol for internet of mobile things:Movement prediction approach',Future Generation Computer systems,Vol 93,pp 822-832.

[15]. Mohamad Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni(2018), 'Bubbles of Trust: A Decentralised blockchain-based authentication system for IoT', Computers and Security, Vol 78, pp 126-142.

[16]. Nejc Rozman, Rok Vrabic, Marko Corn, Tomaz Pozrl, Janez Diaci(2019), 'Distributed Logistics platform based on Blockchain and IoT',Procedia CIRP, Vol 81, pp 826-831.

[17]. Riya Thakore, Rajkumar Vaghashiya, Chintan Patel, Nishant Doshi(2019), 'Blockchain based IoT: A survey',Procedia Computer Science, Vol 155, pp 704-709.

[18]. Rizwan Hamid Randhawa, Abdul Hameed, Ahdnan Noor Mian(2019), 'Energy efficient cross-layer approach for object security of CoAP for IoT devices',Ad Hoc Network,Vol 92,pp 101-761.

[19]. Sakthivel.T, Chandrasekaran.R.M(2018), 'A Dummy Packet –Based Hybrid Security Framework for Mitigating Routing Misbehavior in Multi-Hop Wireless Networks', Wireless Personal Network, Vol 101,pp 1581-1681.

[20]. Somayye Hajiheidari , Karzan Wakil, Maryam Badri, Nima Jafari Navimipour(2019), 'Intrusion system detection in the Internet of things:A comprehensive investigation',Computer Networks,Vol 160,pp 165-191.

[21]. Gholamreza Ramezan, Cyril Leung (2018), 'A Block chain Based Contractual Routing Protocol for the Internet of Things Using Smart Contract', Wireless communication and mobile computing,Vol 2018,pp 14 .

[22]. Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, Usman Ali Shah (2018), 'SIT: A Lightweight Encryption Algorithm For Secure Internet of Things', International Journal Of Advanced Computer Science and Applications, Vol 8.

[23]. Gopal, S.B., Poongodi, C., Nanthiya, D, Divya, E., Aarthy, N (2018), 'Enhancement of routing protocol for low power lossy network for internet of things ', Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018.

[24]. Gopal, S.B., Poongodi, C., Joseph Auxilius Jude, M (2020), Minimum energy consumption objective function for RPL in internet of things', International Journal of Scientific and Technology Research, Vol 9.

[25]. Nanthiya, D., Keerthika, P., Gopal, S.B. (2020), 'Anticipation of wormhole attacks by selective routing in wireless sensor networks', International Journal of Scientific and Technology Research, Vol 9.